UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/631,023	07/30/2003	Glenn F. Evans	MS1-1345USC1	9514

22801 7590 12/07/2006

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 12/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/631,023	EVANS ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/23/2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-94* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-94* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 September 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/10-23-2006*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Applicant's arguments/amendments with respect to amended claims 53 & 71 and previously presented claims 1-52, 54-70, & 72-94 filed 10/23/2006 have been fully considered but they are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Arguments

Regarding claim 1, Applicants list several limitations that they believe are not taught by the combination of Nason and Garcia. Firstly, Applicants contend that "a cryptographic processor that resides on the video card" is not disclosed by either of the cited references. Examiner respectfully disagrees. Garcia, being one of ordinary skill in the art prior to the time this invention was made, clearly stated motivation for incorporating a cryptographic processor to reside on the video card to carry out various encryption/decryption operations (par. 3, lines 15-22). Furthermore, in the cited passage, Garcia suggests that one would be motivated to modify Nason to incorporate the cryptographic processor into the video card to allow for carrying out cryptographic functions at a low cost, as well as more easily. Therefore, Garcia suggests a cryptographic processor that resides on the video card. Secondly, Applicants contend that the cited prior arts fail to teach/suggest "a graphics processor unit (GPU) that resides on the video card." Examiner respectfully disagrees. Nason teaches the GPU operates on the VRAM to allow for projections (par. 49 and fig. 3, elements 302 and 303). Therefore, Nason teaches a GPU that resides on the video card. Thirdly, Applicants contend that the cited prior arts fail to teach/suggest "performing an operation on the decrypted data using the GPU to provide resultant

data." Examiner respectfully disagrees. Nason teaches wherein the valid data in decrypted form is displayed. In this case, displaying the data by projecting is interpreted as the operation being performed on the decrypted data where the resultant data is the data as displayed (par. 56, lines 22-25 and par. 58, lines 9-10). Therefore, Nason teaches performing an operation on the decrypted data using the GPU to provide resultant data. Fourthly, Applicants contend that the cited prior arts of record fail to teach/suggest "re-encrypting, under the influence of the cryptographic processor, the resultant data." Examiner respectfully disagrees. Nason teaches that the valid data is re-obfuscated, i.e. re-encrypted, after being scanned/copied out for projections where the resultant data is that which has been scanned/copied for display (par. 58, lines 9-13 and par. 59, lines 15-20). Thus, Nason teaches re-encrypting, under the influence of the cryptographic processor, the resultant data. Finally, Applicants contend that the cited prior art fails to teach/suggest "at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis." Examiner respectfully disagrees. Nason teaches that various portions of the frame buffer, i.e. portions of a cache, are obfuscated but de-obfuscated for display and then re-obfuscated, i.e. re-encrypted, after being displayed (par. 56, lines 2-15 and par. 58, lines 9-13). Thus, Nason teaches at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis.

Regarding claim 12, Applicants list several limitations that they believe are not taught by the combination of Nason and Garcia. Firstly, Applicants contend that "a cryptographic processor that resides on the video card" is not disclosed by either of the cited references. Examiner respectfully disagrees. Garcia, being one of ordinary skill in the art prior to the time this invention was made, clearly stated motivation for incorporating a cryptographic processor to

reside on the video card to carry out various encryption/decryption operations (par. 3, lines 15-22). Furthermore, in the cited passage, Garcia suggests that one would be motivated to modify Nason to incorporate the cryptographic processor into the video card to allow for carrying out cryptographic functions at a low cost, as well as more easily. Therefore, Garcia suggests a cryptographic processor that resides on the video card. Secondly, Applicants contend that the cited prior arts fail to teach/suggest "a graphics processor unit (GPU) that resides on the video card." Examiner respectfully disagrees. Nason teaches the GPU operates on the VRAM to allow for projections (par. 49 and fig. 3, elements 302 and 303). Therefore, Nason teaches a GPU that resides on the video card. Thirdly, Applicants contend that the cited prior arts fail to teach/suggest "performing an operation on the decrypted data using the GPU to provide resultant data." Examiner respectfully disagrees. Nason teaches wherein the valid data in decrypted form is displayed. In this case, displaying the data by projecting is interpreted as the operation being performed on the decrypted data where the resultant data is the data as displayed (par. 56, lines 22-25 and par. 58, lines 9-10). Therefore, Nason teaches performing an operation on the decrypted data using the GPU to provide resultant data. Fourthly, Applicants contend that the cited prior arts of record fail to teach/suggest "re-encrypting, under the influence of the cryptographic processor, the resultant data." Examiner respectfully disagrees. Nason teaches that the valid data is re-obfuscated, i.e. re-encrypted, after being scanned/copied out for projections where the resultant data is that which has been scanned/copied for display (par. 58, lines 9-13 and par. 59, lines 15-20). Thus, Nason teaches re-encrypting, under the influence of the cryptographic processor, the resultant data. Fifthly, Applicants contend that the cited prior art fails to teach/suggest "writing the encrypted resultant data to a memory surface associated

with the video card." Examiner respectfully disagrees. Nason teaches that after a projection, the data is written back in encrypted form in order to re-obfuscate the secure portion of the frame buffer (par. 59, lines 15-20). Therefore, Nason teaches writing the encrypted resultant data to a video card memory surface associated with the video card. Finally, Applicants contend that the cited prior art fails to teach/suggest "at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis." Examiner respectfully disagrees. Nason teaches that various portions of the frame buffer, i.e. portions of a cache, are obfuscated but de-obfuscated for display and then re-obfuscated, i.e. re-encrypted, after being displayed (par. 56, lines 2-15 and par. 58, lines 9-13). Thus, Nason teaches at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis.

Regarding claim 23, Applicants list several limitations that they believe are not taught by Nason. Firstly, Applicants contend that the prior arts of record fail to teach/suggest "performing an operation on the decrypted data using the GPU to provide resultant data." Examiner respectfully disagrees. Nason teaches wherein the valid data in decrypted form is displayed. In this case, displaying the data by projecting is interpreted as the operation being performed on the decrypted data where the resultant data is the data as displayed (par. 56, lines 22-25 and par. 58, lines 9-10). Therefore, Nason teaches performing an operation on the decrypted data using the GPU to provide resultant data. Secondly, Applicants contend that the cited prior arts of record fail to teach/suggest "re-encrypting the resultant data." Examiner respectfully disagrees. Nason teaches that the valid data is re-obfuscated, i.e. re-encrypted, after being scanned/copied out for projections where the resultant data is that which has been scanned/copied for display (par. 58, lines 9-13 and par. 59, lines 15-20). Thus, Nason teaches re-encrypting the resultant data.

Thirdly, Applicants contend that the cited prior art fails to teach/suggest "writing the encrypted resultant data to a memory surface associated with the video card." Examiner respectfully disagrees. Nason teaches that after a projection, the data is written back in encrypted form in order to re-obfuscate the secure portion of the frame buffer (par. 59, lines 15-20). Therefore, Nason teaches writing the encrypted resultant data to a video card memory surface associated with the video card. Finally, Applicants contend that the cited prior art fails to teach/suggest "at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis." Examiner respectfully disagrees. Nason teaches that various portions of the frame buffer, i.e. portions of a cache, are obfuscated but de-obfuscated for display and then re-obfuscated, i.e. re-encrypted, after being displayed (par. 56, lines 2-15 and par. 58, lines 9-13). Thus, Nason teaches at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis.

Regarding claim 31, Applicants list several limitations that they believe are not taught by the combination of Nason and Garcia. Firstly, Applicants contend that the prior arts of record fail to teach/suggest "performing an operation on the decrypted data using the GPU to provide resultant data." Examiner respectfully disagrees. Nason teaches wherein the valid data in decrypted form is displayed. In this case, displaying the data by projecting is interpreted as the operation being performed on the decrypted data where the resultant data is the data as displayed (par. 56, lines 22-25 and par. 58, lines 9-10). Therefore, Nason teaches performing an operation on the decrypted data using the GPU to provide resultant data. Secondly, Applicants contend that the cited prior arts of record fail to teach/suggest "re-encrypting the resultant data." Examiner respectfully disagrees. Nason teaches that the valid data is re-obfuscated, i.e. re-encrypted, after being scanned/copied out for projections where the resultant data is that which

has been scanned/copied for display (par. 58, lines 9-13 and par. 59, lines 15-20). Thus, Nason teaches re-encrypting the resultant data. Thirdly, Applicants contend that the cited prior art fails to teach/suggest "writing the encrypted resultant data to a memory surface associated with the video card." Examiner respectfully disagrees. Nason teaches that after a projection, the data is written back in encrypted form in order to re-obfuscate the secure portion of the frame buffer (par. 59, lines 15-20). Therefore, Nason teaches writing the encrypted resultant data to a video card memory surface associated with the video card. Finally, Applicants contend that the cited prior art fails to teach/suggest "said acts of decrypting and re-encrypting taking place on a per cache page basis." Examiner respectfully disagrees. Nason teaches that various portions of the frame buffer, i.e. portions of a cache, are obfuscated but de-obfuscated for display and then re-obfuscated, i.e. re-encrypted, after being displayed (par. 56, lines 2-15 and par. 58, lines 9-13). Thus, Nason teaches said acts of decrypting and re-encrypting taking place on a per cache page basis.

Regarding claim 39, Applicants list several limitations that they believe are not taught by Nason. Firstly, Applicants contend that the cited prior art fails to teach "means for decrypting, on a per cache basis, encrypted data that resides on one or more memory surfaces of a video card memory only when an operation is to be performed on the data by a GPU that resides on a video card." Examiner respectfully disagrees. Nason teaches that the GPU decrypts data held in the buffers only before being displayed and that the GPU operates on the VRAM to allow for projections (par. 49; par. 57; and fig. 3, elements 302 and 303). Nason further teaches that various portions of the frame buffer, i.e. portions of a cache, are obfuscated but de-obfuscated for display and then re-obfuscated, i.e. re-encrypted, after being displayed (par. 56, lines 2-15 and

par. 58, lines 9-13). Therefore, Nason teaches means for decrypting, on a per cache basis, encrypted data that resides on one or more memory surfaces of a video card memory only when an operation is to be performed on the data by a GPU that resides on a video card. Secondly, Applicants contend that the prior arts of record fail to teach/suggest "performing an operation on the decrypted data using the GPU to provide resultant data." Examiner respectfully disagrees. Nason teaches wherein the valid data in decrypted form is displayed. In this case, displaying the data by projecting is interpreted as the operation being performed on the decrypted data where the resultant data is the data as displayed (par. 56, lines 22-25 and par. 58, lines 9-10). Therefore, Nason teaches performing an operation on the decrypted data using the GPU to provide resultant data. Thirdly, Applicants contend that the cited prior arts of record fail to teach/suggest "re-encrypting the resultant data." Examiner respectfully disagrees. Nason teaches that the valid data is re-obfuscated, i.e. re-encrypted, after being scanned/copied out for projections where the resultant data is that which has been scanned/copied for display (par. 58, lines 9-13 and par. 59, lines 15-20). Thus, Nason teaches re-encrypting the resultant data. Fourthly, Applicants contend that the cited prior art fails to teach/suggest "writing the encrypted resultant data to a memory surface associated with the video card." Examiner respectfully disagrees. Nason teaches that after a projection, the data is written back in encrypted form in order to re-obfuscate the secure portion of the frame buffer (par. 59, lines 15-20). Therefore, Nason teaches writing the encrypted resultant data to a video card memory surface associated with the video card. Finally, Applicants contend that the cited prior art fails to teach/suggest "at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis." Examiner respectfully disagrees. Nason teaches that various portions of the frame buffer, i.e.

portions of a cache, are obfuscated but de-obfuscated for display and then re-obfuscated, i.e. re-encrypted, after being displayed (par. 56, lines 2-15 and par. 58, lines 9-13). Thus, Nason teaches at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis.

Regarding claim 45, Applicants list several limitations that they believe are not taught by the combination of Nason and Garcia. Firstly, Applicants contend that the cited prior arts fail to teach/suggest "a memory on the video card comprising…one or more output memory surfaces configured to hold encrypted resultant data." Examiner respectfully disagrees. Nason teaches the GPU operates on the VRAM to allow for projections (par. 49 and fig. 3, elements 302 and 303). Furthermore, Nason teaches that this memory holds the valid data to be displayed, i.e. on one or more output memory surfaces (par. 53). Therefore, Nason teaches a memory on the video card comprising…one or more output memory surfaces configured to hold encrypted resultant data. Secondly, Applicants contend that "a cryptographic processor on the video card and configured to control encryption and decryption on the video card" is not disclosed by either of the cited references. Examiner respectfully disagrees. Garcia, being one of ordinary skill in the art prior to the time this invention was made, clearly stated motivation for incorporating a cryptographic processor to reside on the video card to carry out various encryption/decryption operations (par. 3, lines 15-22). Furthermore, in the cited passage, Garcia suggests that one would be motivated to modify Nason to incorporate the cryptographic processor into the video card to allow for carrying out cryptographic functions at a low cost, as well as more easily. Therefore, Garcia suggests a cryptographic processor on the video card and configured to control encryption and decryption on the video card. Finally, Applicants contend that neither reference teaches/suggests "the cryptographic processor further being configured to enable data that has

been operated upon by the GPU to be encrypted, on a per cache basis, to an output memory surface." Examiner respectfully disagrees. Nason teaches that once the data has been displayed it will be re-encrypted and is subsequently stored in encrypted format (par. 57 and par. 59, lines 15-20). Furthermore, Nason teaches that various portions of the frame buffer, i.e. portions of a cache, are obfuscated but de-obfuscated for display and then re-obfuscated, i.e. re-encrypted, after being displayed (par. 56, lines 2-15 and par. 58, lines 9-13). Thus, Nason teaches the cryptographic processor further being configured to enable data that has been operated upon by the GPU to be encrypted, on a per cache basis, to an output memory surface.

Regarding claim 53, Applicants list several limitations that they believe are not taught by the combination of Nason and Strasser. First, Applicants contend that the cited prior arts fail to teach/suggest "associating, with each input memory surface, a decryptor that is uniquely configured so as to decrypt the encrypted data that is held by the associated input memory surface." Examiner respectfully disagrees. Strasser, as one of ordinary skill in the art prior to the time the invention was made, teaches that each video segment is associated with its own encryption/decryption key (col. 2, lines 1-12). Therefore, it would have been obvious to modify Nason to include this advantage in order to combat a brute force attack which may be launched to gain access to the video content. Thus, Strasser suggests motivation for modifying Nason to include associating, with each input memory surface, a decryptor that is uniquely configured so as to decrypt the encrypted data that is held by the associated input memory surface. Second, Applicants contend that Nason fails to teach, "performing an operation on the decrypted data using the GPU to provide resultant data." Examiner respectfully disagrees. Nason teaches wherein the valid data in decrypted form is displayed. In this case, displaying the data by

projecting is interpreted as the operation being performed on the decrypted data where the resultant data is the data as displayed (par. 56, lines 22-25 and par. 58, lines 9-10). Therefore, Nason teaches performing an operation on the decrypted data using the GPU to provide resultant data. Third, Applicants contend that the cited prior arts of record fail to teach/suggest "re-encrypting the resultant data." Examiner respectfully disagrees. Nason teaches that the valid data is re-obfuscated, i.e. re-encrypted, after being scanned/copied out for projections where the resultant data is that which has been scanned/copied for display (par. 58, lines 9-13 and par. 59, lines 15-20). Thus, Nason teaches re-encrypting the resultant data. Finally, Applicants also contend that the cited prior arts of record fail to teach/suggest "writing the encrypted resultant data to an output memory surface associated with the video card, at least one of said acts of decrypting and re-encrypting taking place on a per cache basis." Examiner respectfully disagrees. Nason teaches the GPU operates on the VRAM to allow for projections (par. 49 and fig. 3, elements 302 and 303). Furthermore, Nason teaches that this memory holds the valid data to be displayed, i.e. on one or more output memory surfaces (par. 53). Yet further, Nason teaches that various portions of the frame buffer, i.e. portions of a cache, are obfuscated but de-obfuscated for display and then re-obfuscated, i.e. re-encrypted, after being displayed (par. 56, lines 2-15 and par. 58, lines 9-13). Thus, Nason teaches writing the encrypted resultant data to an output memory surface associated with the video card, at least one of said acts of decrypting and re-encrypting taking place on a per cache basis.

Regarding claim 70, Applicants list several limitations that they believe are not taught by the combination of Nason and Strasser. First, Applicants contend that the cited prior arts fail to teach/suggest "associating, with each input memory surface, a decryptor that is uniquely

configured so as to decrypt the encrypted data that is held by the associated input memory surface." Examiner respectfully disagrees. Strasser, as one of ordinary skill in the art prior to the time the invention was made, teaches that each video segment is associated with its own encryption/decryption key (col. 2, lines 1-12). Therefore, it would have been obvious to modify Nason to include this advantage in order to combat a brute force attack which may be launched to gain access to the video content. Thus, Strasser suggests motivation for modifying Nason to include associating, with each input memory surface, a decryptor that is uniquely configured so as to decrypt the encrypted data that is held by the associated input memory surface. Second, Applicants contend that Nason fails to teach, "performing an operation on the decrypted data using the GPU to provide resultant data." Examiner respectfully disagrees. Nason teaches wherein the valid data in decrypted form is displayed. In this case, displaying the data by projecting is interpreted as the operation being performed on the decrypted data where the resultant data is the data as displayed (par. 56, lines 22-25 and par. 58, lines 9-10). Therefore, Nason teaches performing an operation on the decrypted data using the GPU to provide resultant data. Third, Applicants contend that the cited prior arts of record fail to teach/suggest "re-encrypting the resultant data." Examiner respectfully disagrees. Nason teaches that the valid data is re-obfuscated, i.e. re-encrypted, after being scanned/copied out for projections where the resultant data is that which has been scanned/copied for display (par. 58, lines 9-13 and par. 59, lines 15-20). Thus, Nason teaches re-encrypting the resultant data. Finally, Applicants also contend that the cited prior arts of record fail to teach/suggest "writing the encrypted resultant data to an output memory surface associated with the video card, said acts of decrypting and re-encrypting taking place on a per cache basis." Examiner respectfully disagrees. Nason teaches

the GPU operates on the VRAM to allow for projections (par. 49 and fig. 3, elements 302 and 303). Furthermore, Nason teaches that this memory holds the valid data to be displayed, i.e. on one or more output memory surfaces (par. 53). Yet further, Nason teaches that various portions of the frame buffer, i.e. portions of a cache, are obfuscated but de-obfuscated for display and then re-obfuscated, i.e. re-encrypted, after being displayed (par. 56, lines 2-15 and par. 58, lines 9-13). Thus, Nason teaches writing the encrypted resultant data to an output memory surface associated with the video card, said acts of decrypting and re-encrypting taking place on a per cache basis.

Regarding claim 87, Applicants list several limitations that they believe are not taught by the combination of Nason, Strasser, and Garcia. Firstly, Applicants contend that the cited prior arts fail to teach/suggest "a graphics processor unit (GPU) on the video card." Examiner respectfully disagrees. Nason teaches the GPU operates on the VRAM to allow for projections (par. 49 and fig. 3, elements 302 and 303). Therefore, Nason teaches a GPU on the video card. Secondly, Applicants contend that "a cryptographic processor on the video card and configured to control encryption and decryption on the video card" is not disclosed by either of the cited references. Examiner respectfully disagrees. Garcia, being one of ordinary skill in the art prior to the time this invention was made, clearly stated motivation for incorporating a cryptographic processor to reside on the video card to carry out various encryption/decryption operations (par. 3, lines 15-22). Furthermore, in the cited passage, Garcia suggests that one would be motivated to modify Nason to incorporate the cryptographic processor into the video card to allow for carrying out cryptographic functions at a low cost, as well as more easily. Therefore, Garcia suggests a cryptographic processor on the video card and configured to control encryption and

decryption on the video card. Thirdly, Applicants contend that the cited prior arts of record fails to teach "the cryptographic processor comprising a key manager for managing keys that can be utilized for encrypting and decrypting data on the video card." Examiner respectfully disagrees. Strasser suggests that the use of keys unique to each stream for content encryption/decryption protects the content from eavesdroppers (col. 3, line 59 – col. 4, line 10). Furthermore, in order to ensure proper encryption/decryption there must be some type of function which manages the keys used per data stream (col. 4, lines 16-26). Therefore, Strasser suggests the cryptographic processor comprising a key manager for managing keys that can be utilized for encrypting and decrypting data on the video card." Fourthly, Applicants contend that neither reference teaches/suggests "the cryptographic processor further being configured to enable data that has been operated upon by the GPU to be encrypted to an output memory surface." Examiner respectfully disagrees. Nason teaches that once the data has been displayed it will be re-encrypted and is subsequently stored in encrypted format (par. 57 and par. 59, lines 15-20). Thus, Nason teaches the cryptographic processor further being configured to enable data that has been operated upon by the GPU to be encrypted to an output memory surface. Finally, Applicants contend that the cited prior arts of record fail to teach/suggest "data that has been operated upon by a GPU to be encrypted on a per cache page basis." Examiner respectfully disagrees. Nason teaches that various portions of the frame buffer, i.e. portions of a cache, are obfuscated but de-obfuscated for display and then re-obfuscated, i.e. re-encrypted, after being displayed (par. 56, lines 2-15 and par. 58, lines 9-13). Thus, Nason teaches data that has been operated upon by a GPU to be encrypted on a per cache page basis.

Due to the reasons stated above, the Examiner maintains rejections with respect to amended claims 53 & 71 and previously presented claims 1-52, 54-70, & 72-94. Nason teaches the limitations that the Applicant suggests distinguish from the prior art. Furthermore, Garcia and/or Strasser in combination with Nason teach the limitations not explicitly disclosed by Nason. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 102

I. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

II. Claim 23, 26-27, 30-31, 34-35, 38-39, 41, and 44 are rejected under 35 U.S.C. 102(e) as being fully anticipated by Nason et al., US Pub. No. 2005/0102264.

As per claims 23 and 39:

Nason et al. teach a method/system comprising: decrypting encrypted data that resides on one or more memory surfaces of a video card memory, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card (par. 56-57); performing an operation on the decrypted data using the GPU to provide resultant data (par. 56); re-encrypting the resultant data (par. 59); and writing the encrypted resultant data to a video card memory surface associated with the video card (par. 59),

at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis (par. 56).

As per claim 26:

Nason et al. teach the method of claim 23, wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis (par. 57).

As per claim 27:

Nason et al. teach the method of claim 23, wherein the acts of decrypting are performed using at least one key that was received from a trusted software component (par. 55).

As per claim 30:

Nason et al. teach the method of claim 23, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed (par. 56).

As per claim 31:

Nason et al. teach a method comprising: decrypting encrypted data that resides on one or more memory surfaces of a video card memory, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card (par. 56-57); performing an operation on the decrypted data using the GPU to provide resultant data (par. 56); re-encrypting the resultant data (par. 59); and writing the encrypted resultant data to a video card memory surface associated with the video card (par. 59), said acts of decrypting and re-encrypting taking place on a per cache page basis (par. 56).

As per claim 34:

Nason et al. teach the method of claim 31, wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis (par. 57).

As per claim 35:

Nason et al. teach the method of claim 31, wherein the acts of decrypting are performed using at least one key that was received from a trusted software component (par. 55).

As per claim 38:

Nason et al. teach the method of claim 31, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed (par. 56).

As per claim 41:

Nason et al. teach the system of claim 39, wherein the means for performing comprises a GPU (par. 56-57).

As per claim 44:

Nason et al. teach the system of claim 39, further comprising means for pooling decrypted pages to avoid multiple decryptions of a page that might be needed more than once (par. 56).

Claim Rejections - 35 USC § 103

III. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

IV. Claims 1-2, 5-8, 11-13, 16-20, 22, 40, 42, 45, 48-50, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nason et al., US Pub. No. 2005/0102264 and further in view of Garcia, US Pub. No. 2002/0136408.

As per claim 1:

Nason et al. substantially teach a method comprising: decrypting encrypted data that resides on one or more memory surfaces associated with a video card, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card (par. 56-57); performing an operation on the decrypted data using the GPU to provide resultant data (par. 56); re-encrypting, under the influence of the cryptographic processor, the resultant data (par. 59); and writing the encrypted resultant data to a memory surface associated with the video card (par. 59); at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis (par. 56).

Not explicitly disclosed is said act of decrypting being performed under the influence of a cryptographic processor that resides on the video card. However, Garcia teaches that incorporating cryptographic capabilities within the GPU has many added benefits (par. 3). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to incorporate the cryptographic processor within the GPU which is located on the graphics card. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Garcia suggests that incorporating cryptographic capabilities within the GPU makes performing cryptographic functions easier and is not costly in par. 3, lines 15-22.

As per claim 2:

Nason et al. and Garcia substantially teach the method of claim 1. Furthermore, Nason et al. teach wherein the memory surfaces reside on the video card (par. 56).

As per claim 5:

Nason et al. and Garcia substantially teach the method of claim 1. Furthermore, Nason et al. teach wherein the act of decrypting and re-encrypting take place on a pixel-by-pixel basis (par. 57).

As per claim 6:

Nason et al. and Garcia substantially teach the method of claim 1. Furthermore, Garcia teaches wherein the cryptographic processor comprises a hardware component mounted on the video card (par. 3).

As per claim 7:

Nason et al. and Garcia substantially teach the method of claim 1. Furthermore, Garcia teaches wherein the cryptographic processor comprises an integrated circuit chip mounted on the video card (par. 3).

As per claim 8:

Nason et al. and Garcia substantially teach the method of claim 1. Furthermore, Nason et al. teach wherein the cryptographic processor comprises a trusted component (par. 53).

As per claim 11:

Nason et al. and Garcia substantially teach the method of claim 1. Furthermore, Nason et al. teach wherein the act of decrypting comprises caching decrypted pages in a local page pool

cache to avoid multiple decryptions if a same page is needed (par. 56).

As per claim 12:

Nason et al. substantially teach a method comprising: decrypting encrypted data that resides on one or more memory surfaces associated with a video card, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card (par. 56-57); performing an operation on the decrypted data using the GPU to provide resultant data (par. 56); re-encrypting, under the influence of the cryptographic processor, the resultant data (par. 59); and writing the encrypted resultant data to a memory surface associated with the video card (par. 59); said acts of decrypting and re-encrypting taking place on a per cache page basis (par. 56).

Not explicitly disclosed is said act of decrypting being performed under the influence of a cryptographic processor that resides on the video card. However, Garcia teaches that incorporating cryptographic capabilities within the GPU has many added benefits (par. 3). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to incorporate the cryptographic processor within the GPU which is located on the graphics card. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Garcia suggests that incorporating cryptographic capabilities within the GPU makes performing cryptographic functions easier and is not costly in par. 3, lines 15-22.

As per claim 13:

Nason et al. and Garcia substantially teach the method of claim 12. Furthermore, Nason et al. teach wherein the memory surfaces reside on the video card (par. 56).

As per claim 16:

Nason et al. and Garcia substantially teach the method of claim 12. Furthermore, Nason et al. teach wherein the act of decrypting and re-encrypting take place on a pixel-by-pixel basis (par. 57).

As per claim 17:

Nason et al. and Garcia substantially teach the method of claim 12. Furthermore, Garcia teaches wherein the cryptographic processor comprises a hardware component mounted on the video card (par. 3).

As per claim 18:

Nason et al. and Garcia substantially teach the method of claim 12. Furthermore, Garcia teaches wherein the cryptographic processor comprises an integrated circuit chip mounted on the video card (par. 3).

As per claim 19:

Nason et al. and Garcia substantially teach the method of claim 12. Furthermore, Nason et al. teach wherein the cryptographic processor comprises a trusted component (par. 53).

As per claim 22:

Nason et al. and Garcia substantially teach the method of claim 12 Furthermore, Nason et al. teach wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed (par. 56).

As per claim 40:

Nason et al. teach the system of claim 39. Not explicitly disclosed is wherein the means for decrypting comprises, at least in part, cryptographic hardware inside the GPU. However, Garcia teaches that incorporating cryptographic capabilities within the GPU has many added benefits (par. 3). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to incorporate the cryptographic processor within the GPU which is located on the graphics card. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Garcia suggests that incorporating cryptographic capabilities within the GPU makes performing cryptographic functions easier and is not costly in par. 3, lines 15-22.

As per claim 42:

Nason et al. substantially teach the system of claim 39. Not explicitly disclosed is wherein the means for re-encrypting comprises, at least in part, cryptographic processor hardware mounted on the video card. However, Garcia teaches that incorporating cryptographic capabilities within the GPU has many added benefits (par. 3). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to incorporate the cryptographic processor within the GPU which is located on the graphics card. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Garcia suggests that incorporating cryptographic capabilities within the GPU makes performing cryptographic functions easier and is not costly in par. 3, lines 15-22.

As per claims 45 and 52:

Nason et al. substantially teach a system comprising: a video card (par. 56); a graphics processor unit (GPU) on the video card and configured to process video data that is to be rendered on a display device (par. 57); memory on the video card comprising one or more input memory surfaces configured to hold encrypted data that is to be operated upon by the GPU (par. 52), and one or more output memory surfaces configured to hold encrypted resultant data that is to be rendered on the display device (par. 53); a means being configured to enable encrypted data on one or more of the input memory surfaces to be decrypted, on a per cache page basis (par. 56), in connection with an operation that is to be performed on the data by the GPU (par. 53); and the cryptographic processor further being configured to enable data that has been operated upon by the GPU to be encrypted, on a per cache page basis (par. 56), to an output memory surface (par. 57).

Not explicitly disclosed is a cryptographic processor on the video card configured to control encryption and decryption (as well as the other specified functions) on the video card. However, Garcia teaches that incorporating cryptographic capabilities within the GPU has many added benefits (par. 3). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to incorporate the cryptographic processor within the GPU which is located on the graphics card. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Garcia suggests that incorporating cryptographic capabilities within the GPU makes performing cryptographic functions easier and is not costly in par. 3, lines 15-22.

As per claim 48:

Nason et al. and Garcia substantially teach the system of claim 45. Furthermore, Garcia teaches wherein the cryptographic processor comprises a hardware component mounted on the video card (par. 3).

As per claim 49:

Nason et al. and Garcia substantially teach the system of claim 45. Furthermore, Garcia teaches wherein the cryptographic processor comprises an integrated circuit chip (par. 3).

As per claim 50:

Nason et al. and Garcia substantially teach the system of claim 45. Furthermore, Nason et al. teach wherein the cryptographic processor comprises a trusted component (par. 53).

V. Claims 3-4, 14-15, and 46-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nason et al., US Pub. No. 2005/0102264 and Garcia, US Pub. No. 2002/0136408, as applied to claims 1, 12, and 45 above, and further in view of Ritter, US Patent No. 5,727,062.

As per claim 3:

Nason et al. and Garcia substantially teach the method of claim 1. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages (col. 9, lines 46-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use block ciphers to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into

existing environments in col. 9, lines 46-52.

As per claim 4:

Nason et al. and Garcia substantially teach the method of claim 1. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages over fixed-size block ciphers (col. 9, lines 40-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use variable block ciphers where the size of the block is associated with a cache line of a cache page in order to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 40-52.

As per claim 14:

Nason et al. and Garcia substantially teach the method of claim 12. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages (col. 9, lines 46-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use block ciphers to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the

time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 46-52.

As per claim 15:

Nason et al. and Garcia et al. substantially teach the method of claim 12. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages over fixed-size block ciphers (col. 9, lines 40-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use variable block ciphers where the size of the block is associated with a cache line of a cache page in order to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 40-52.

As per claim 46:

Nason et al. and Garcia substantially teach the system of claim 45. Not explicitly disclosed is the method wherein the cryptographic processor is configured to use block ciphers to effect encryption and decryption. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages (col. 9, lines 46-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the

method disclosed in Nason et al. to use block ciphers to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 46-52.

As per claim 47:

Nason et al. and Garcia substantially teach the system of claim 45. Not explicitly disclosed is the method wherein the cryptographic processor is configured to use one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages over fixed-size block ciphers (col. 9, lines 40-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use variable block ciphers where the size of the block is associated with a cache line of a cache page in order to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 40-52.

VI. Claims 9-10 and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nason et al., US Pub. No. 2005/0102264 and Garcia, US Pub. No. 2002/0136408, as applied to claims 1 and 12 above, and further in view of Mical et al., US Patent No. 5,572,235.

As per claim 9:

Nason et al. and Garcia substantially teach the method of claim 1. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data in order to translate the XY values to a system memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also disclosed. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Mical et al. suggest that using the spryte-rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

As per claim 10:

Nason et al. and Garcia substantially teach the method of claim 1. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data in order to translate the XY values to a system memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also disclosed. Yet further, Mical et al. teach that the data is transmitted via a D-bus (col.8, lines 42-54). Therefore, it would have been

obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data by trusted software and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Mical et al. suggest that using the spryte-rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

As per claim 20:

Nason et al. and Garcia substantially teach the method of claim 12. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data in order to translate the XY values to a system memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also disclosed. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Mical et al. suggest that using the spryte-rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

As per claim 21:

Nason et al. and Garcia substantially teach the method of claim 12. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data in order to translate the XY values to a system memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also disclosed. Yet further, Mical et al. teach that the data is transmitted via a D-bus (col.8, lines 42-54). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data by trusted software and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Mical et al. suggest that using the spryte-rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

VII. Claims 24-25, 32-33, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nason et al., US Pub. No. 2005/0102264, as applied to claims 23, 31, and 39 above, and further in view of Ritter, US Patent No. 5,727,062.

As per claim 24:

Nason et al. substantially teach the method of claim 23. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers. However, Ritter teaches variable size block ciphers that can be used for encryption and

decryption with great advantages (col. 9, lines 46-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use block ciphers to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 46-52.

As per claim 25:

Nason et al. substantially teach the method of claim 23. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages over fixed-size block ciphers (col. 9, lines 40-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use variable block ciphers where the size of the block is associated with a cache line of a cache page in order to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 40-52.

As per claim 32:

Nason et al. substantially teach the method of claim 31. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages (col. 9, lines 46-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use block ciphers to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 46-52.

As per claim 33:

Nason et al. substantially teach the method of claim 31. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages over fixed-size block ciphers (col. 9, lines 40-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use variable block ciphers where the size of the block is associated with a cache line of a cache page in order to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into

existing environments in col. 9, lines 40-52.

As per claim 43:

Nason et al. substantially teach the system of claim 39. Not explicitly disclosed is the method wherein said means for decrypting and re-encrypting comprise one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages over fixed-size block ciphers (col. 9, lines 40-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use variable block ciphers where the size of the block is associated with a cache line of a cache page in order to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 40-52.

VII. Claims 28-29 and 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nason et al., US Pub. No. 2005/0102264, as applied to claim 23 and 31 above, and further in view of Mical et al., US Patent No. 5,572,235.

As per claim 28:

Nason et al. substantially teach the method of claim 23. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data in order to translate the XY values to a system

memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also disclosed. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Mical et al. suggest that using the spryte-rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

As per claim 29:

Nason et al. substantially teach the method of claim 23. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data in order to translate the XY values to a system memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also disclosed. Yet further, Mical et al. teach that the data is transmitted via a D-bus (col.8, lines 42-54). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data by trusted software and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made,

made, would have been motivated to do so since Mical et al. suggest that using the spryte-rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

As per claim 36:

Nason et al. substantially teach the method of claim 31. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data in order to translate the XY values to a system memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also disclosed. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Mical et al. suggest that using the spryte-rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

As per claim 37:

Nason et al. substantially teach the method of claim 31. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data

in order to translate the XY values to a system memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also disclosed. Yet further, Mical et al. teach that the data is transmitted via a D-bus (col.8, lines 42-54). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data by trusted software and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Mical et al. suggest that using the spryte-rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

VIII. Claim 51 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nason et al., US Pub. No. 2005/0102264 and Garcia, US Pub. No. 2002/0136408, as applied to claim 45 above, further in view of Strasser et al., US Patent No. 6,934,389.

As per claim 51:

Nason et al. and Garcia substantially teach the system of claim 45. Not explicitly disclosed is the method wherein the cryptographic processor is configured to set up a session key with a trusted software component. However, Strasser et al teach that using keys which are unique to each data stream for content encryption/decryption protects the content from eavesdroppers (col. 3, line 59 – col. 4, line 10). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use session keys for encrypting the content and to communicate the key used between the

trusted software component and the cryptographic processor. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Strasser et al. suggest that changing the keys constantly and using different keys is the best defense against a brute-force attack in col. 2, lines 1-12.

IX. Claim 53-56, 59, 63-66, 69-73, 76, 80-83, and 86 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nason et al., US Pub. No. 2005/0102264 and further in view of Strasser et al., US Patent No. 6,934,389.

As per claim 53:

Nason et al. substantially teach a method comprising: providing multiple input memory surfaces that are to hold encrypted data that is to be processed by a graphics processor unit (GPU) on a video card (par. 55); performing an operation on the decrypted data using the GPU to provide resultant data (par. 56); re-encrypting the resultant data (par. 59); and writing the encrypted resultant data to an output memory surface associated with the video card (par. 59), at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis (par. 56).

Not explicitly disclosed is associating, with each input memory surface, a decryptor that is uniquely able to decrypt the encrypted data that is held by the associated input memory surface; decrypting, with at least one associated decryptor, encrypted data that resides on at least one respective input memory surface. However, Strasser et al teach that using keys which are unique to each data stream for content encryption/decryption protects the content from eavesdroppers (col. 3, line 59 – col. 4, line 10). Therefore, it would have been obvious to a

person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use a decryptor, that is unique to each of the input memory surfaces, to decrypt the content which is encrypted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Strasser et al. suggest that changing the keys constantly and using different keys is the best defense against a brute-force attack in col. 2, lines 1-12.

As per claim 54:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Furthermore, Nason et al. teach wherein the act of providing the multiple input memory surfaces comprises providing at least one input memory surface on the video card (par. 55).

As per claim 55:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Not explicitly disclosed is wherein the act of re-encrypting comprises using an encryptor that is uniquely associated with the output memory surface to re-encrypt the resultant data. However, Nason et al. teach re-encrypting the data for storage (par. 59). Furthermore, Strasser et al teach that using keys which are unique to each data stream for content encryption/decryption protects the content from eavesdroppers (col. 3, line 59 – col. 4, line 10). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use an encryptor, that is unique to each of the output memory surfaces, to re-encrypt the resultant data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Strasser et al. suggest that changing the using different keys for various data portions is the best

defense against a brute-force attack in col. 2, lines 1-12.

As per claim 56:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Furthermore, Strasser et al. teach wherein the negotiated key indices are used to identify and regulate which keys are used in decrypt operations (col. 10, lines 13-27). Not explicitly disclosed is wherein the act of re-encrypting comprises using an encryptor that is uniquely associated with the output memory surface to re-encrypt the resultant data. However, Nason et al. teach re-encrypting the data for storage (par. 59). Furthermore, Strasser et al teach that using keys which are unique to each data stream for content encryption/ decryption protects the content from eavesdroppers (col. 3, line 59 – col. 4, line 10). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use an encryptor, that is unique to each of the output memory surfaces, to re-encrypt the resultant data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Strasser et al. suggest that changing the using different keys for various data portions is the best defense against a brute-force attack in col. 2, lines 1-12.

As per claim 59:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Furthermore, Nason et al. teach wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis (par. 57).

As per claim 63:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Furthermore, Nason et al. teach wherein the act of decrypting is performed only when the GPU is to perform an operation on data that resides on a particular input memory surface (par. 50).

As per claim 64:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Furthermore, Nason et al. teach the method further comprising restricting one or more operations that can be performed by the GPU based on whether encrypted output is available (par. 56).

As per claim 65:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Furthermore, Nason et al. teach the method further comprising decrypting the encrypted resultant data for rendering on a display device (par. 57).

As per claim 66:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Furthermore, Nason et al. teach the method further comprising decrypting, with a display convertor, the encrypted resultant data for rendering on a display device (par. 57).

As per claim 69:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Furthermore, Nason et al. teach wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed (par. 56).

As per claim 70:

Nason et al. substantially teach a method comprising: providing multiple input memory surfaces that are to hold encrypted data that is to be processed by a graphics processor unit

(GPU) on a video card (par. 55); performing an operation on the decrypted data using the GPU to provide resultant data (par. 56); re-encrypting the resultant data (par. 59); and writing the encrypted resultant data to an output memory surface associated with the video card (par. 59), said acts of decrypting and re-encrypting taking place on a per cache page basis (par. 56).

Not explicitly disclosed is associating, with each input memory surface, a decryptor that is uniquely able to decrypt the encrypted data that is held by the associated input memory surface; decrypting, with at least one associated decryptor, encrypted data that resides on at least one respective input memory surface. However, Strasser et al teach that using keys which are unique to each data stream for content encryption/decryption protects the content from eavesdroppers (col. 3, line 59 – col. 4, line 10). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use a decryptor, that is unique to each of the input memory surfaces, to decrypt the content which is encrypted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Strasser et al. suggest that changing the keys constantly and using different keys is the best defense against a brute-force attack in col. 2, lines 1-12.

As per claim 71:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Furthermore, Nason et al. teach wherein the act of providing the multiple input memory surfaces comprises providing at least one input memory surface on the video card (par. 55).

As per claim 72:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Not explicitly disclosed is wherein the act of re-encrypting comprises using an encryptor that is uniquely associated with the output memory surface to re-encrypt the resultant data. However, Nason et al. teach re-encrypting the data for storage (par. 59). Furthermore, Strasser et al teach that using keys which are unique to each data stream for content encryption/decryption protects the content from eavesdroppers (col. 3, line 59 – col. 4, line 10). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use an encryptor, that is unique to each of the output memory surfaces, to re-encrypt the resultant data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Strasser et al. suggest that changing the using different keys for various data portions is the best defense against a brute-force attack in col. 2, lines 1-12.

As per claim 73:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Furthermore, Strasser et al. teach wherein the negotiated key indices are used to identify and regulate which keys are used in decrypt operations (col. 10, lines 13-27). Not explicitly disclosed is wherein the act of re-encrypting comprises using an encryptor that is uniquely associated with the output memory surface to re-encrypt the resultant data. However, Nason et al. teach re-encrypting the data for storage (par. 59). Furthermore, Strasser et al teach that using keys which are unique to each data stream for content encryption/decryption protects the content from eavesdroppers (col. 3, line 59 – col. 4, line 10). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use an encryptor,

that is unique to each of the output memory surfaces, to re-encrypt the resultant data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Strasser et al. suggest that changing the using different keys for various data portions is the best defense against a brute-force attack in col. 2, lines 1-12.

As per claim 76:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Furthermore, Nason et al. teach wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis (par. 57).

As per claim 80:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Furthermore, Nason et al. teach wherein the act of decrypting is performed only when the GPU is to perform an operation on data that resides on a particular input memory surface (par. 50).

As per claim 81:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Furthermore, Nason et al. teach the method further comprising restricting one or more operations that can be performed by the GPU based on whether encrypted output is available (par. 56).

As per claim 82:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Furthermore, Nason et al. teach the method further comprising decrypting the encrypted resultant data for rendering on a display device (par. 57).

As per claim 83:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Furthermore, Nason et al. teach the method further comprising decrypting, with a display convertor, the encrypted resultant data for rendering on a display device (par. 57).

As per claim 86:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Furthermore, Nason et al. teach wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed (par. 56).

X. Claims 87, 89-92, and 93-94 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nason et al., US Pub. No. 2005/0102264, Garcia, US Pub. No. 2002/0136408, and further in view of Strasser et al., US Patent No. 6,934,389.

As per claims 87 and 94:

Nason et al. substantially teach a system comprising: a video card (par. 56); a graphics processor unit (GPU) on the video card and configured to process video data that is to be rendered on a display device (par. 57); memory on the video card comprising one or more input memory surfaces configured to hold encrypted data that is to be operated upon by the GPU (par. 52), and one or more output memory surfaces configured to hold encrypted resultant data that is to be rendered on the display device (par. 53); the cryptographic processor being configured to enable encrypted data on one or more of the input memory surfaces to be decrypted on a per cache page basis (par. 56) so that the decrypted data can be operated upon by the GPU (par. 53); the cryptographic processor further being configured to enable data that has been operated upon by the GPU to be encrypted on a per cache page basis to an output memory surface (par. 57).

Not explicitly disclosed is a cryptographic processor on the video card and configured to control encryption and decryption on the video card. However, Garcia teaches that incorporating cryptographic capabilities within the GPU has many added benefits (par. 3). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to incorporate the cryptographic processor within the GPU which is located on the graphics card. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Garcia suggests that incorporating cryptographic capabilities within the GPU makes performing cryptographic functions easier and is not costly in par. 3, lines 15-22.

Also not explicitly disclosed is the cryptographic processor comprising a key manager for managing keys that can be utilized for encrypting and decrypting data on the video card; and each individual input memory surface having its own unique associated key for decrypting encrypted data held thereon. However, Strasser et al teach that using keys which are unique to each data stream for content encryption/decryption protects the content from eavesdroppers (col. 3, line 59 – col. 4, line 10). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use a decryptor, that is unique to each of the input memory surfaces, to decrypt the content which is encrypted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Strasser et al. suggest that changing the keys constantly and using different keys is the best defense against a brute-force attack in col. 2, lines 1-12.

As per claim 89:

Nason et al., Garcia, and Strasser et al. substantially teach the system of claim 87. Furthermore, Nason et al. wherein encryption and decryption takes place on a pixel-by-pixel basis (par. 57).

As per claim 90:

Nason et al., Garcia, and Strasser et al. substantially teach the system of claim 87. Furthermore, Nason et al. teach wherein encrypted data held on an input memory surface is decrypted only when it is to be operated upon by the GPU (par. 56).

As per claim 91:

Nason et al., Garcia, and Strasser et al. substantially teach the system of claim 87. Furthermore, Garcia teaches wherein the cryptographic processor comprises an integrated circuit chip (par. 3).

As per claim 92:

Nason et al., Garcia, and Strasser et al. substantially teach the system of claim 87. Furthermore, Nason et al. teach wherein the cryptographic processor comprises a trusted component (par. 53).

As per claim 93:

Nason et al., Garcia, and Strasser et al. substantially teach the system of claim 87. Not explicitly disclosed is wherein the cryptographic processor is configured to set up a session key with a trusted software component. However, Strasser et al teach that using keys which are unique to each data stream for content encryption/decryption protects the content from eavesdroppers (col. 3, line 59 – col. 4, line 10). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et

al. to use session keys for encrypting the content and to communicate the key used between the trusted software component and the cryptographic processor. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Strasser et al. suggest that changing the keys constantly and using different keys is the best defense against a brute-force attack in col. 2, lines 1-12.

XI. Claims 57-58, 74-75, and 88 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nason et al., US Pub. No. 2005/0102264 and Strasser et al., US Patent No. 6,934,389, as applied to claims 53, 70, and 87 above, and further in view of Ritter, US Patent No. 5,727,062.

As per claim 57:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages (col. 9, lines 46-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use block ciphers to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 46-52.

As per claim 58:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages over fixed-size block ciphers (col. 9, lines 40-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use variable block ciphers where the size of the block is associated with a cache line of a cache page in order to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 40-52.

As per claim 74:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages (col. 9, lines 46-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use block ciphers to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into

existing environments in col. 9, lines 46-52.

As per claim 75:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Not explicitly disclosed is the method wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages over fixed-size block ciphers (col. 9, lines 40-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use variable block ciphers where the size of the block is associated with a cache line of a cache page in order to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 40-52.

As per claim 88:

Nason et al., Garcia, and Strasser et al. substantially teach the system of claim 87. Not explicitly disclosed is wherein the cryptographic processor is configured to control encryption and decryption using block ciphers. However, Ritter teaches variable size block ciphers that can be used for encryption and decryption with great advantages (col. 9, lines 46-52). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to use block ciphers to decrypt and re-encrypt the data. This modification would have been obvious because a person having ordinary skill in the art, at the

time the invention was made, would have been motivated to do so since Ritter suggests that using variable size block ciphers has advantages such as higher speed and being a better fit into existing environments in col. 9, lines 46-52.

XII. Claims 60-62 and 77-79 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nason et al., US Pub. No. 2005/0102264 and Strasser et al., US Patent No. 6,934,389, as applied to claims 70 above, and further in view of Garcia, US Pub. No. 2002/0136408.

As per claim 60:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Not explicitly disclosed is wherein the acts of decrypting and re-encrypting are performed under the influence of a cryptographic processor that resides on the video card. However, Garcia teaches that incorporating cryptographic capabilities within the GPU has many added benefits (par. 3). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to incorporate the cryptographic processor within the GPU which is located on the graphics card. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Garcia suggests that incorporating cryptographic capabilities within the GPU makes performing cryptographic functions easier and is not costly in par. 3, lines 15-22.

As per claim 61:

Nason et al., Strasser et al., and Garcia substantially teach the method of claim 60. Furthermore, Garcia teaches wherein the cryptographic processor comprises an integrated circuit

chip (par. 3).

As per claim 62:

Nason et al., Strasser et al., and Garcia substantially teach the method of claim 60. Furthermore, Nason et al. teach wherein the cryptographic processor comprises a trusted component (par. 53).

As per claim 77:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Not explicitly disclosed is wherein the acts of decrypting and re-encrypting are performed under the influence of a cryptographic processor that resides on the video card. However, Garcia teaches that incorporating cryptographic capabilities within the GPU has many added benefits (par. 3). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to incorporate the cryptographic processor within the GPU which is located on the graphics card. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Garcia suggests that incorporating cryptographic capabilities within the GPU makes performing cryptographic functions easier and is not costly in par. 3, lines 15-22.

As per claim 78:

Nason et al., Strasser et al., and Garcia substantially teach the method of claim 77. Furthermore, Garcia teaches wherein the cryptographic processor comprises an integrated circuit chip (par. 3).

As per claim 79:

Nason et al., Strasser et al., and Garcia substantially teach the method of claim 77. Furthermore, Nason et al. teach wherein the cryptographic processor comprises a trusted component (par. 53).

XIII. Claims 67-68 and 84-85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nason et al., US Pub. No. 2005/0102264 and Strasser et al., US Patent No. 6,934,389, as applied to claims 53 and 70 above, and further in view of Mical et al., US Patent No. 5,572,235.

As per claim 67:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the input memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data in order to translate the XY values to a system memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also disclosed. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Mical et al. suggest that using the spryte-rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

As per claim 68:

Nason et al. and Strasser et al. substantially teach the method of claim 53. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the input memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data in order to translate the XY values to a system memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also disclosed. Yet further, Mical et al. teach that the data is transmitted via a D-bus (col.8, lines 42-54). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data by trusted software and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Mical et al. suggest that using the spryte-rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

As per claim 84:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the input memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data in order to translate the XY values to a system memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also

disclosed. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Mical et al. suggest that using the spryte-rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

As per claim 85:

Nason et al. and Strasser et al. substantially teach the method of claim 70. Not explicitly disclosed is the method further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the input memory surfaces. However, Mical et al. teach the use of various flag fields communicated with the data in order to translate the XY values to a system memory address (col. 13, Table 1.1, B21 = YOXY"). Furthermore, these flag bits control the way that the content is to be rendered in accordance with the spryte-rendering engine that is also disclosed. Yet further, Mical et al. teach that the data is transmitted via a D-bus (col.8, lines 42-54). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Nason et al. to receive pre-swizzled encrypted data by trusted software and write the pre-swizzled encrypted data to the one or more memory surfaces. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Mical et al. suggest that using the spryte-

rendering engine has an advantage over conventional methods where time and memory are wasted in col. 10, lines 31-52.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi
Nadia Khoshnoodi
Examiner
Art Unit 2137
12/4/2006

NK

E Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER